On page 48, replace the emboldened heading on the top of the page under the title with:

ABSTRACT

On page 48 replace the abstract with the following paragraph:

> The present invention provides encryption schemes and apparatus which securely generate a cipher-text which in itself contains checks for assuring message integrity. It also provides compatible decryption schemes confirming message integrity. The encryption scheme generates a cipher-text with message integrity in a single pass with little additional computational cost, while retaining at least the same level of security as schemes based on a MAC. One embodiment encrypts a plain-text message by dividing the plain-text message into a multitude of plain-text blocks and encrypting the plain-text blocks to form a multitude of cipher-text blocks. A single pass technique is used in this process to embed a message integrity check in the cipher-text block. A message integrity check is embedded in the cipher-text blocks by embedding a set of pseudo random numbers, which may be dependent, but are pair-wise differentially uniform. We also describe an embodiment which is highly parallelizable.